

## VERIFICATION CONTROL SYSTEM

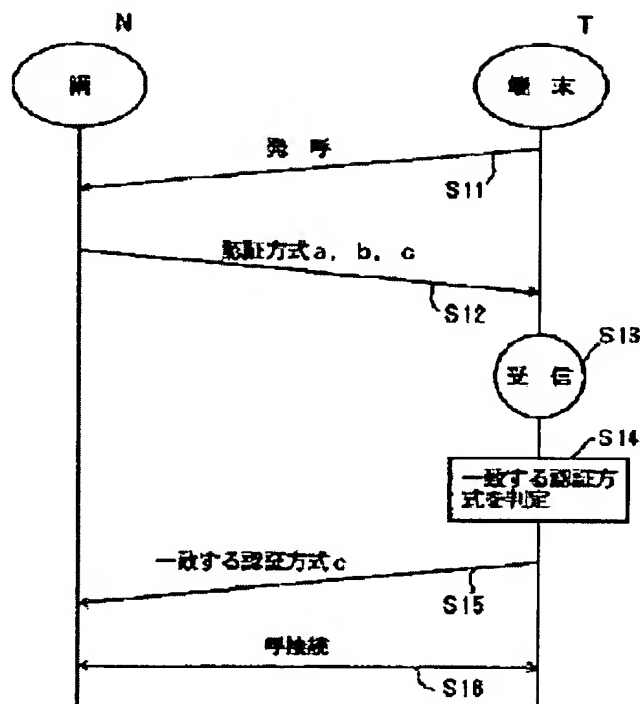
**Patent number:** JP6261033  
**Publication date:** 1994-09-16  
**Inventor:** SHIMADA MASAKI; others: 02  
**Applicant:** NIPPON TELEGR & TELEPH CORP  
**Classification:**  
 - international: H04L9/00; H04L9/10; H04L9/12; G09C1/00  
 - european:  
**Application number:** JP19930046984 19930308  
**Priority number(s):**

### Abstract of JP6261033

**PURPOSE:** To allow a network to simply decide the verification system without notifying the verification system of a terminal equipment by providing plural verification means to the network, selecting one of them and informing the selected system to the terminal equipment and allowing the terminal equipment to select one of the executable verification systems when it is included in the notice and giving a reply to the network.

**CONSTITUTION:** A terminal equipment T makes a call to a network N. Upon the receipt of a connection request from the terminal equipment T, the network N sends information about verification systems a-c possessed by the network N to the terminal equipment T.

The terminal equipment T discriminates whether or not a system coincident with the verification system of its own is in existence among the verification systems noticed from the network N. When there is any coincident verification system, the terminal equipment T informs the verification system to the network N. Since the verification system noticed from the terminal equipment T is coincident with that informed from the network N, the network N verifies the terminal equipment T and the network N and the terminal equipment T are interconnected.



Data supplied from the esp@cenet database - Patent Abstracts of Japan

(19)日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11)特許出願公開番号

特開平6-261033

(43)公開日 平成 6年(1994) 9月16日

(51)Int.Cl. <sup>5</sup>	識別記号	庁内整理番号	F I	技術表示箇所
H 0 4 L 9/00				
9/10				
9/12				
G 0 9 C 1/00		8837-5L		
		7117-5K		
			H 0 4 L 9/ 00	Z
			審査請求 未請求	請求項の数 1 O L (全 7 頁)

(21)出願番号 特願平5-46984

(22)出願日 平成 5年(1993) 3月 8日

(71)出願人 000004226

日本電信電話株式会社

東京都千代田区内幸町一丁目 1 番 6 号

(72)発明者 嶋田 勝紀

東京都千代田区内幸町 1 丁目 1 番 6 号 日  
本電信電話株式会社内

(72)発明者 前田 潤二

東京都千代田区内幸町 1 丁目 1 番 6 号 日  
本電信電話株式会社内

(72)発明者 舟川 公敏

東京都千代田区内幸町 1 丁目 1 番 6 号 日  
本電信電話株式会社内

(74)代理人 弁理士 伊東 忠彦

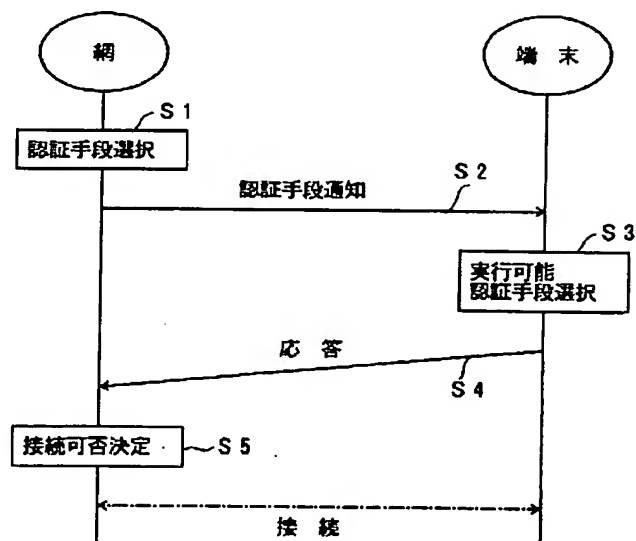
(54)【発明の名称】 認証制御方式

(57)【要約】

【目的】 本発明の目的は、網が端末のもつ認証方式を意識することなしに、簡易に認証方式を決定することができる認証制御方式を提供することである。

【構成】 本発明は、網が端末を認証するための複数の認証手段を有し、認証手段から少なくとも1つの認証手段を選択して(ステップ1)、端末に通知し(ステップ2)、端末が網からの該通知の中に実行可能な認証手段が含まれる場合に、認証手段のうち1つを選択して(ステップ3)網に応答し(ステップ4)、網が端末間の認証手段が同一であるか判断し(ステップ5)、等しければ網と端末間を接続可能とする(ステップ6)。

本発明の原理説明図



## 【特許請求の範囲】

【請求項1】 端末との接続時に該端末の認証を行う網と、認証手段を具備する端末とを含む通信システムにおける認証制御方式において、

該網は端末を認証するための複数の認証手段を有し、該認証手段から少なくとも1つの認証手段を選択して、該端末に通知し、

該端末は該網からの該通知の中に実行可能な認証手段が含まれる場合に、該認証手段のうち1つを選択して該網に応答し、

該網は該端末間の該認証手段が同一であるか判断し、等しければ該網と該端末間を接続可能であると認証することを特徴とする認証制御方式。

## 【発明の詳細な説明】

## 【0001】

【産業上の利用分野】本発明は認証制御方式に係り、特に通信におけるセキュリティの保護のために網側から端末の正当性をチェックするための認証を必要とする通信システムの認証制御方式に関する。

## 【0002】

【従来の技術】従来の第1の認証を行う方式を説明する。移动通信方式に必要な認証を行う方式として、文献“花岡、尾上、上林、「デジタル移动通信網における認証方式」電子情報通信学会、秋期全国大会、pp. 2-232、1990年”がある。この方法は、認証を行うユーザ間で共有される秘密の暗号鍵K1を用いて、認証起動側のユーザから適当な平文と鍵K1を用いた暗号文Cを送信し、被認証側ユーザは受信した平文から暗号鍵K1を用いて暗号文C'を生成し、認証起動側ユーザに返送する。ここで、暗号文CとC'が等しければ認証ができたことになる。

【0003】次に従来の第2の認証を行う方式を説明する。図6は従来の第2の認証方式の一例を示すブロック図である。同図において、網N1は認証方式aを有し、網N2は認証方式bを有する。また、端末T1は認証方式のaを有し、端末T2は認証方式bを有する。

【0004】このとき、同一の認証方式を具備する端末T1と網N1との間では、

- ①端末T1が網N1に接続を要求すると、
- ②網N1が認証鍵により決定される認証情報を端末T1に送信し、端末T1に認証を要求する。
- ③端末T1は、網N1からの認証情報に対応する認証応答情報を含む応答を網N1に応答する。
- ④網N1が認証応答情報の正当性を確認した後に、端末T1の接続を確認する。

【0005】一方、同図において、点線で示される関係のように、網Nと端末T間の具備する認証方式が異なる場合には、網Nと端末T間の認証は許容されない。従って、異なる認証では接続されないためにセキュリティが守られる。

【0006】ここで、認証方式aを具備する端末T1と、認証方式bを採用する網N2があるとする。この端末T1と網N2間の接続を可能とするためには、網N2と端末T1の何れかが複数の認証方式を具備する必要がある。例えば、網N2が端末T1の正当性を認証により確認するためには、網N2の指定した認証方式に端末T1が従うものとし、網N2に指定された認証方式を端末T1が備えていれば認証が成立する。

【0007】そのため、異なる認証方式を採用している複数の通信システムにおいて、同一の端末が利用可能とするためには、相互接続を可能とするシステム間で互いの認証方式を具備しなければならない。

【0008】図7は従来の第2の認証方式における網のメモリを示す。同図に示すように網は各端末毎に具備している認証方式11をメモリ10内に記憶する。同図の例では、端末T1が有する認証方式はa、端末T2が有する認証方式はb、端末T3が有する認証方式はaというように、認証方式を各端末毎に具備する。例えば、網Nが端末Tに対してメモリ10に記憶してあるメモリ内情報11（認証方式）よりbを通知して、端末からbの認証方式が通知されれば網Nは端末Tを認証する。

【0009】また、網との接続を希望する端末が網の認証方式を具備する方式もある。図8は従来の第2の認証方式における端末が有する認証方式を示す。同図において、端末は接続を希望する網の認証方式を具備するものとする。

【0010】同図の例では、この端末の端末内メモリ20が有するメモリ内情報21（認証方式）は、方式a、方式b、方式c等である。ここで、網Nから方式aが通知された場合には認証され、網Nから認証方式としてdが通知された場合には、この端末には、認証方式dが具備されていないので、認証されない。

## 【0011】

【発明が解決しようとする課題】しかしながら、上記第1の従来の方式では、暗号鍵等を予め設定して認証側及び被認証側でそれぞれ同じ暗号鍵を保持するため、鍵の変更時に、認証側で暗号鍵を変更しても被認証側で変更が終了しておらず、鍵に矛盾が発生することがある。この場合には、暗号文が認証側と被認証側で一致することがないために認証が成功しない。また、鍵を第3者により悪用されることも考えられる。

【0012】また、上記第2の方式では、網が認証すべき端末毎の認証方式を記憶するためには、端末数に見合う記憶領域を必要とし、端末で複数の認証方式を持つ方式では、後で網の利用を要求するシステムが増加した場合に認証方式の追加が困難である。

【0013】本発明は上記の点に鑑みなされたもので、上記従来の問題点を解決し、網が端末のもつ認証方式を意識することなしに、網と端末の間での交渉により簡易に認証方式を決定することができる認証制御方式を提供

することを目的とする。

【0014】

【課題を解決するための手段】図1は本発明の原理説明図である。

【0015】端末との接続時に該端末の認証を行う網と、認証手段を具備する端末とを含む通信システムにおける認証制御方式において、網は端末を認証するための複数の認証手段を有し、認証手段から少なくとも1つの認証手段を選択して（ステップ1）、端末に通知し（ステップ2）、端末は網からの通知の中に実行可能な認証手段が含まれる場合に、認証手段のうち1つを選択して（ステップ3）網に応答し（ステップ4）、網は端末間の認証手段が同一であるか判断し（ステップ5）、等しければ網と端末間を接続可能であると認証する（ステップ6）。

【0016】

【作用】本発明は、網に認証方式を複数持たせ、端末は網の持つ認証方式のうち何れかを持つことにより、網が端末の持つ認証方式を意識せずに、認証方式を端末に通知する。端末は網からの1つの認証方式に限定されることがなく、自端末が有している認証方式が網から通知された認証方式に含まれていれば、網に接続要求を行うことができる。一方、端末が保持していない認証方式で網にアクセスしても網は接続を許可しないため、通信のセキュリティを保つことができる。

【0017】

【実施例】以下、図面により本発明の実施例を説明する。

【0018】図2は本発明の第1の実施例のブロック構成図である。同図において、網Nは複数の認証方式a、b、cを有し、端末Tは認証方式c、dを有する。このような関連において、網Nと端末Tの接続の認証について説明する。

【0019】図3は本発明の第1の実施例の処理のタイミングチャートである。

【0020】ステップ11）まず、最初に端末Tが網Nに対して発呼する（または、網Nから着呼）。

【0021】ステップ12）網Nは端末Tからの接続要求を受信すると、端末Tに対して、網Nが有する認証方式a、b、cを送出する。

【0022】ステップ13）端末Tは網Nからの認証方式a、b、cを受信する。

【0023】ステップ14）端末Tは網Nからの認証方式のうち、自端末に有する認証方式と一致する方式があるかを判定する。

【0024】ステップ15）ステップ4において、一致する認証方式が有る場合には、その認証方式を網Nに送信する。この例の場合には、認証方式cが一致しているので、網Nに認証方式cを送出する。

【0025】ステップ16）これにより、網Nでは認証

方式cが一致しているために端末Tを認証し、網Nと端末Tが接続される。

【0026】また、端末Tが認証方式d、cを有している場合には、網Nから通知した認証方式には認証方式d、eは含まれていないため、認証されない。

【0027】次に、本発明の第2の実施例として、予め認証強度により認証方式を決定する場合について説明する。本実施例では、認証強度に対応する認証方式を用いる方式について説明する。

【0028】図4は本発明の第2の実施例の認証方式の設定を説明するための図である。同図において、網Nまたは端末Tの認証設定部40と、網Nから端末T、または端末Tから網Nに対しての通信を行うためのインターフェース部50から構成される。認証設定部40は、バッファメモリ41、強度比較部42、認証方式テーブル作成部43、認証方式テーブル44により構成される。

【0029】本実施例における認証方式に設定は、まず、網Nまたは端末Tの認証設定部40に重要度に基づいた認証強度が入力され、一旦入力された認証強度をバッファメモリ41に蓄える。次に、強度比較部42において、先に入力された認証強度との比較を行い、強度が大きい順にバッファメモリ41にソートしておく。認証方式テーブル作成部43は、最高強度のものを強度1とし、認証方式aとする。さらに、2番目の強度のものを強度2とし、認証方式bとする。同様に3番目の強度のものを強度3とし、認証方式cとする。このように強度に対応する認証方式を認証方式テーブル44に設定する。

【0030】例えば、網Nはインターフェース部50により端末Nから接続要求があった場合に、このように認証方式テーブル44に設定された認証方式を読みだして端末Tに通知する。上記認証方式の設定は、網N側、端末T側共に予め設定されるものとする。

【0031】図5は本発明の第2の実施例の網及び端末の認証方式を示す。網Nには強度1を認証方式a、強度2を認証方式b、強度3を認証方式cとして設定されている。また、端末Tは、強度1を認証方式a、強度3を認証方式cとした2つの認証方式を有している。

【0032】図5における認証について説明する。認証を行うためのシーケンスは図3に示すシーケンスと同様である。以下の説明において、網Nを移動通信における無線回線制御局とし、端末Tを移動局として説明する。

【0033】まず、移動局から無線回線制御局に発呼することにより呼接続要求を行う。接続要求を受信した無線回線制御局は、自局が有する認証方式a、b、cを移動局に通知する。

【0034】移動局は、無線回線制御局から通知された認証方式a、b、cのうち自端末が有する認証方式がその中に含まれているかを判断する。図5の例では、認証方式a、cが含まれているので、その認証方式a、bを

無線回線制御局に送出する。無線回線制御局は、移動局からの通知を受け取ると、同じ認証方式を持つ移動局を認証し、移動局間の呼接続を行う。

【0035】また、移動局が強度2の認証方式b、強度4の認証方式dを有している場合には、移動局は無線回線制御局から通知された認証方式に含まれる認証方式を持たないため、無線回線制御局からの認証は行われない。従って、無線回線制御局間の呼接続は行われない。

【0036】なお、本発明は、網及び端末の両方に複数の認証方式を保持しているが、網側から端末に通知される認証方式が複数であればよく、端末側が常時、複数の認証方式を保持する必要はない。

【0037】なお、本発明は本発明の主旨を逸脱しない範囲で網から端末を認証できる方式であれば、上記実施例に限定されることなく種々変更が可能である。

【0038】

【発明の効果】上述のように本発明の認証制御方式によれば、網が端末の持つ認証方式を意識せずに、認証方式を端末に通知し、端末は網のもつ認証方式のうち何れかを有していれば、網は端末を認証することができる。また、一方、端末側で網から通知された認証方式を持っていない場合には、認証されないため、通信におけるセキュリティを保つことができる。

【0039】また、重要度等、網と端末との関連に応じて認証方式を互いに設定しておくこともできるため、関連重要度の高い順に接続を行うことも可能である。

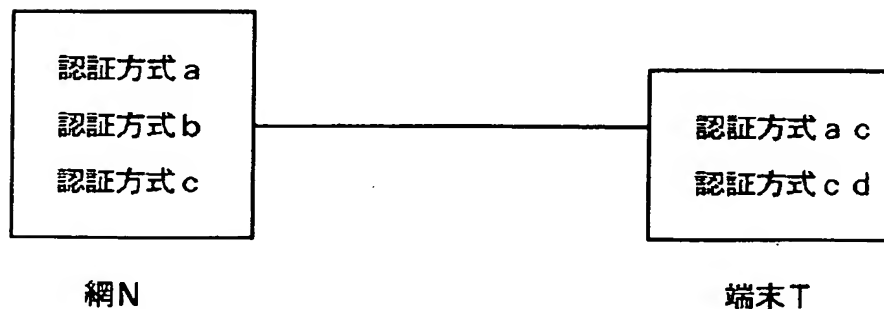
【図面の簡単な説明】

【図1】本発明の原理説明図である。

\*

【図2】

本発明の第1の実施例のブロック構成図



\* 【図2】本発明の第1の実施例のブロック構成図である。

【図3】本発明の第1の実施例の処理のシーケンスチャートである。

【図4】本発明の第2の実施例の認証方式の設定を説明するための図である。

【図5】本発明の第2の実施例の網及び端末の認証方式を示す図である。

【図6】従来の第2の認証方式の一例を示すブロック図である。

【図7】従来の第2の認証方式における網のメモリを示す図である。

【図8】従来の第2の認証方式における端末が有する認証方式を示す図である。

【符号の説明】

N, N1, N2 網

T 端末

10 メモリ

11 メモリ内情報（認証方式）

20 端末メモリ

21 端末メモリ内情報（認証方式）

40 認証設定部

41 バッファメモリ

42 強度比較部

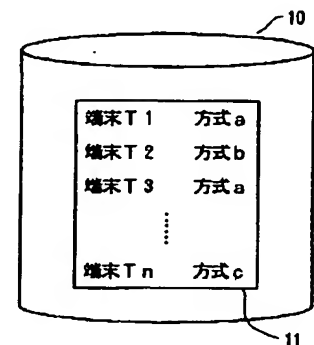
43 認証方式テーブル作成部

44 認証方式テーブル

50 インターフェース部

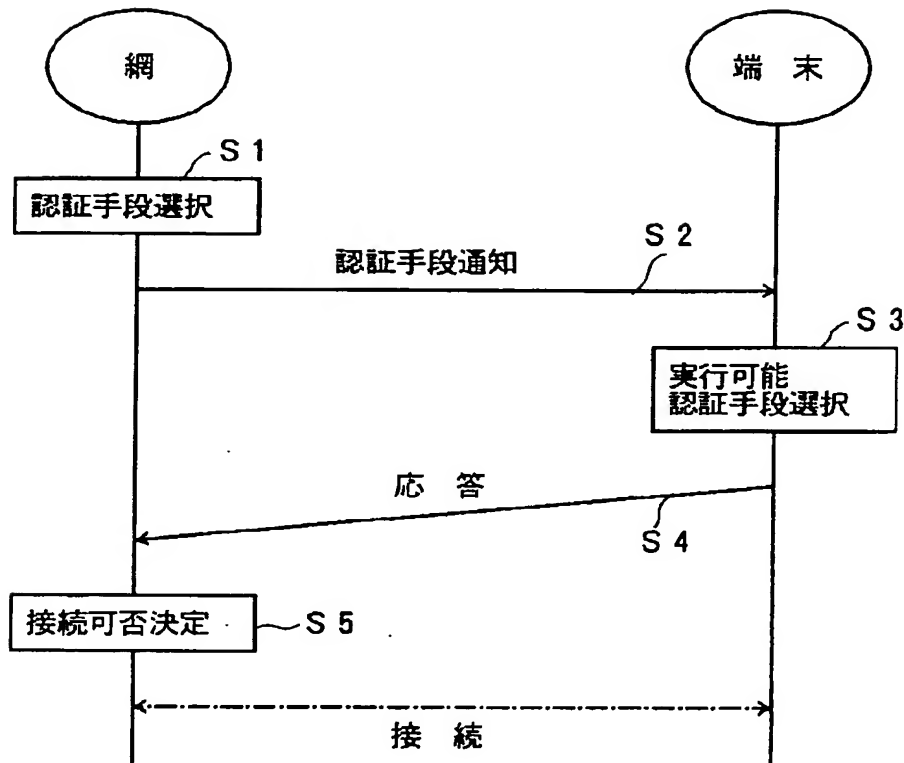
【図7】

従来の第2の認証方式における網のメモリを示す図



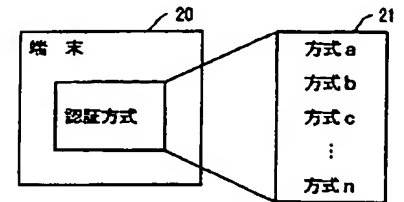
【図 1】

## 本発明の原理説明図



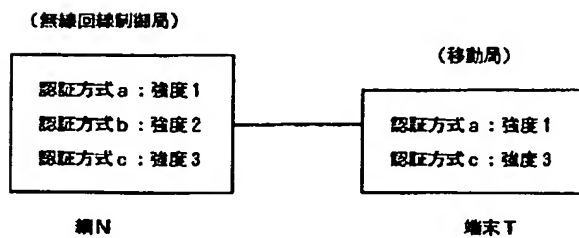
【図 8】

従来の第 2 の認証方式における端末が有する  
認証方式を示す図



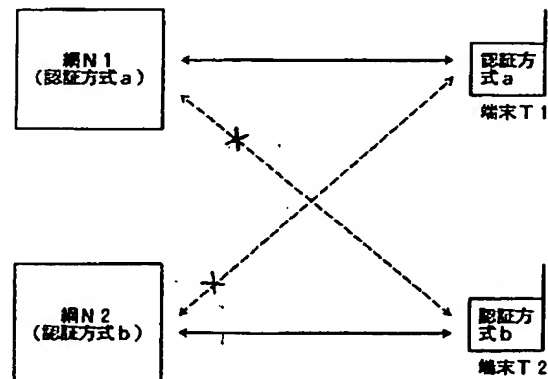
【図 5】

本発明の第 2 の実施例の網及び端末の  
認証方式を示す図



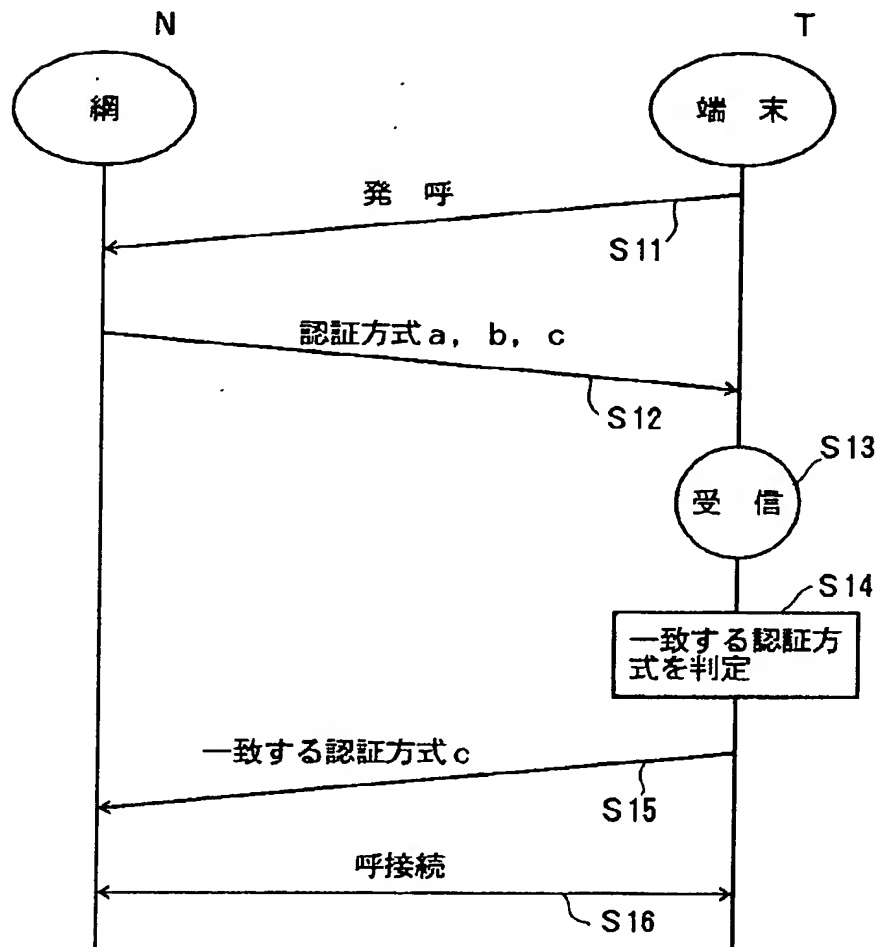
【図 6】

従来の第 2 の認証方式の一例を示すブロック図



【図3】

本発明の第1の実施例の処理のシーケンスチャート



【図 4】

本発明の第 2 の実施例の認証方式設定を  
説明するための図

